

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION**

RACHEAL LOVE, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

GALVESTON COLLEGE,

Defendant.

Case No. 3:23-cv-00367

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Racheal Love (“Plaintiff”) brings this Class Action Petition (“Petition”) against Galveston College (“Galveston” or “Defendant”), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Petition against Galveston for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names and Social Security numbers (collectively, “personally identifiable information” or “PII”).

2. Defendant is a junior college that offers “more than 80 certificate and associate degree programs” to its students.¹

3. Upon information and belief, former and current students, employees, and applicants for admission or employment are required to entrust Defendant with an extensive

¹ <https://www.gc.edu/> (last accessed Oct. 31, 2023).

amount of their PII, used for Defendant’s business, in order to enroll at Galveston or be eligible for employment. Defendant retains this information for at least many years and even after the relationship has ended.

4. On an undisclosed date, Defendant experienced “an incident involving unauthorized access to certain devices within [Galveston’s] network.”² In response, Defendant engaged outside cybersecurity experts to “to conduct an investigation[.]” into the nature and scope of the cyberattack.³ As a result of that investigation, Defendant concluded—on an undisclosed date—that “an unauthorized party intermittently accessed [Galveston’s] network and took certain files from [Galveston’s] servers.”⁴

5. Subsequently, the Akira ransomware group took credit for conducting the cyberattack at Galveston.⁵

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiff’s and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant’s negligent and/or careless acts and omissions and its utter failure to protect students’ sensitive data. Hackers targeted and obtained Plaintiff’s and Class Members’ PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their

² The “Notice Letter”.

³ *Id.*

⁴ *Id.*

⁵ <https://hackmanac.com/news/hacks-of-today-24-25-26-2023> (last accessed Nov. 3, 2023).

respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence, at a minimum, and violates federal and state statutes.

9. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised

through disclosure to an unknown and unauthorized third party.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

12. Plaintiff Racheal Love is a natural person, resident, and a citizen of Galveston, Texas. Defendant obtained and continues to maintain Plaintiff Love's PII, and Defendant owed her a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Love would not have entrusted her PII to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

13. Defendant Galveston College is a Texas-based junior college with its principal place of business located at 4015 Avenue Q, Galveston, Texas 77550.

JURISDICTION AND VENUE

14. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

15. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in the Galveston Division of the Southern District of Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in the Galveston Division of the Southern District of Texas and a

substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District

FACTUAL ALLEGATIONS

Defendant's Business

17. Defendant is a junior college that offers "more than 80 certificate and associate degree programs" to its students.⁶

18. Plaintiff and Class Members are or were students and/or student applicants at Galveston or provided Defendant with the relevant PII for some other purpose (*e.g.*, employment or application for employment or study).

19. To enroll in classes or other programs at Defendant, Plaintiff and Class Members were required to provide sensitive and confidential PII, including but not limited to: their names and Social Security numbers. The same or similar information was provided by other victims of this Data Breach, including employees of Defendant or applicants for employment or admission.

20. Upon information and belief, Defendant made promises and representations to its students, including Plaintiff and Class Members, that the PII collected from them as a condition of enrollment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

21. Indeed, the Identity Theft Program policy posted on Defendant's website provides that:

In order to further prevent the likelihood of identity theft occurring with respect to College accounts, the College will take the following steps with respect to its internal

⁶ <https://www.gc.edu/> (last accessed Oct. 31, 2023).

operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and require and keep only the kinds of customer information that are necessary for College purposes.⁷

22. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

23. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

24. Defendant had obligations created by FTC Act, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

25. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

⁷ <https://gc.edu/wp-content/uploads/2016/10/IdentityTheftPROGRAM.pdf> (last accessed Oct. 31, 2023).

The Data Breach

26. On or about October 16, 2023, Defendant began sending Plaintiff and other victims of the Data Breach an untitled letter (the "Notice Letter") informing them that:

We concluded an investigation into an incident involving unauthorized access to certain devices within our network. When we became aware of the incident, we immediately took affirmative steps to address the issue. Outside cybersecurity experts were engaged to conduct an investigation, and we reported the incident to law enforcement. The investigation determined that an unauthorized party intermittently accessed our network and took certain files from our servers. We then conducted a thorough review of those files and determined that the files contained your name and Social Security number.⁸

27. Since the Data Breach, the Akira ransomware group took credit for conducting the cyberattack at Galveston.⁹

28. Omitted from the Notice Letter were the dates of the Data Breach, the date that Defendant detected the Data Breach, the dates of Defendant's investigation, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

29. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members,

⁸ The Notice Letter.

⁹ <https://hackmanac.com/news/hacks-of-today-24-25-26-2023> (last accessed Nov. 3, 2023).

causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

31. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiff and Class Members, including their names and Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

32. Plaintiff further believes that her PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII , such as encrypting the information or deleting it when it is no longer needed.

34. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁰

35. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF),

¹⁰ How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Oct. 17, 2022).

Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹¹

36. To prevent and detect cyber-attacks or ransomware attacks Defendant could and

¹¹ *Id.* at 3–4.

should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;
- Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹²

37. Given that Defendant was storing the PII of its current and former students, employees, student applicants, and employee applicants, Defendant could and should have

¹² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Oct. 17, 2022).

implemented all of the above measures to prevent and detect cyberattacks.

38. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of, upon information and belief, thousands of individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

39. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

40. As a condition to enroll, apply for enrollment, or obtain employment at Galveston, Plaintiff and Class Members are required to give their sensitive and confidential PII to Defendant. Defendant retains this information even after the relationship has ended and Defendant is no longer required to retain this information.

41. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

43. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

44. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk because Educational Institutions in Possession of PII are Particularly Susceptible to Cyber Attacks

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the breach.

46. Data breaches, including those perpetrated against educational institutions that store PII in their systems, have become widespread.

47. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹³

48. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

49. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly."¹⁴

¹³ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last accessed Oct. 11, 2023).

¹⁴ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

50. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

51. Defendant knew and understood unprotected or exposed PII in the custody of educational institutions, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

52. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

53. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

54. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

55. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

56. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security

numbers—fraudulent use of that information and damage to victims may continue for years.

57. As an educational institution in custody of students’, employees’, and employee applicants’ PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

58. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁵ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁶

59. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁷ For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸ Criminals can also purchase access

¹⁵ 17 C.F.R. § 248.201 (2013).

¹⁶ *Id.*

¹⁷ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

¹⁸ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.

to entire company data breaches from \$900 to \$4,500.¹⁹

60. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁰

61. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly

6, 2017, *available at*: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

¹⁹ *In the Dark*, VPNOverview, 2019, *available at*: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

²⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

inherited into the new Social Security number.”²¹

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number and name.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²²

65. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

66. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future

²¹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).

²² Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

harm.²³

Defendant Fails to Comply with FTC Guidelines

67. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁴

69. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁵

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

²³ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

²⁴ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

²⁵ *Id.*

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. These FTC enforcement actions include actions against educational institutions, like Defendant.

73. Defendant failed to properly implement basic data security practices.

74. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to customers’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

75. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its students, employees, and other personnel. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

76. As noted above, experts studying cyber security routinely entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

77. Several best practices have been identified that a minimum should be implemented by educational institutions in possession of PII, like Defendant, including but not

limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

78. Other best cybersecurity practices that are standard in the higher education industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

79. Upon information and belief Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These foregoing frameworks are existing and applicable industry standards in the higher education industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

81. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft

82. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

83. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

84. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

85. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

86. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

87. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.²⁶

88. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

²⁶ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/) (last visited on May 26, 2023).

89. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

90. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiff and the other Class Members.

91. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

92. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

93. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

94. Galveston’s Notice Letter explicitly instructed Plaintiff and Class Members to take steps to mitigate any harms that may result from the data breach, stating: “[f]or more

information about identity theft protection, additional steps you may consider taking in response, and instructions for how to active your complimentary, one-year IdentityWorks membership, please see the pages that follow this letter.”²⁷

95. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice Letter encourages them to do, monitor their financial accounts for many years to mitigate the risk of identity theft.

96. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

97. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁸

98. Plaintiff’s mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

99. And for those Class Members who experience actual identity theft and fraud, the

²⁷ Notice Letter.

²⁸ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁹

Diminution of Value of PII

100. PII is a valuable property right.³⁰ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

101. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³¹

102. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³²

103. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{33,34} Consumers who agree to provide their web

²⁹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

³⁰ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

³¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sep. 13, 2022).

³² <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³³ <https://datacoup.com/>

³⁴ <https://digi.me/what-is-digime/>

browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁵

104. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

105. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., Social Security numbers and names.

106. The fraudulent activity resulting from the Data Breach may not come to light for years.

107. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

108. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

³⁵ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>

continue to incur such damages in addition to any fraudulent use of their PII.

109. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

110. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable & Necessary

111. Given the type of targeted attack in this case, the sophisticated criminal activity, and the type of PII involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

112. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

113. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

breach, where victims can easily cancel or close credit and debit card accounts.³⁶ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

114. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

115. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

Loss of Benefit of the Bargain

116. Furthermore, Defendant’s poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for educational services or accepting employment from Defendant under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services and/or employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF LOVE'S EXPERIENCE

117. Plaintiff Love is a former Galveston student who attended Galveston in or about 2021.

118. In order to enroll at Galveston, she was required to provide her PII to Defendant,

³⁶ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

including her name and Social Security number.

119. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII in its system, despite no longer being a student at Galveston.

120. Plaintiff Love is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Love would not have provided her PII to Defendant had she known that Defendant would fail to reasonably safeguard that data from unauthorized access.

121. Plaintiff Love received the Notice Letter, by U.S. mail, directly from Defendant, dated October 16, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her full name and Social Security number.

122. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

123. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains

unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

124. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

125. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

126. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

127. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

128. Plaintiff Love has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

129. Plaintiff brings this action on behalf of herself and all other persons similarly situated.

130. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in October 2023 (the "Class").

131. Excluded from the Class are Defendant's officers and directors, and any entity

in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

132. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

133. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals impacted in the Data Breach is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of persons were impacted in the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

134. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- f. Whether Defendant breached its duty to Class Members to safeguard their PII;
- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant was unjustly enriched;
- k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

135. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

136. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent

and experienced in litigating class actions, including data privacy litigation of this kind.

137. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

138. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

139. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

140. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

- a. Whether Defendant failed to timely notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

141. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

142. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

143. Defendant required Plaintiff and Class Members to submit sensitive, non-public, personal information in order to enroll in one of Defendant's classes or programs or be eligible for employment.

144. Defendant's duty of care to use reasonable security measures arose as a result

of the special relationship that existed between Defendant and the individuals that entrusted their PII to Defendant. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from the Data Breach.

145. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to design, implement, and monitor systems, policies, and processes by which it could reasonably prevent and detect a breach of their security systems in a reasonably expeditious period of time.

146. Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with industry standards concerning data security would result in the compromise of that PII — just like the Data Breach that ultimately came to pass.

148. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

149. Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and

necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

150. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

151. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII . The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised; and
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

152. The breach of security was reasonably foreseeable given the known high

frequency of cyberattacks and data breaches generally and in the higher education industry.

153. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

154. Plaintiff and the putative class members had no way to protect themselves from the damage Defendant is responsible for.

155. The imposition of a duty of care on Defendant to safeguard the PII it maintained is appropriate because any social utility of Defendant's conduct—of which little, if any, exists—is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

156. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and unsecure manner.

157. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

158. Plaintiff and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

159. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

160. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

161. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

162. Defendant violated Section 5 of the FTC Act and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

163. Defendant’s violation of Section 5 of the FTC Act and similar state statutes constitutes negligence *per se*.

164. Class members are consumers within the class of persons Section 5 of the FTC Act and similar state statutes were intended to protect.

165. Moreover, the harm that has occurred is the type of harm the FTC Act and

similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

168. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

169. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

170. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

171. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

173. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

THIRD COUNT
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

174. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

175. When Plaintiff and Class Members provided their PII to Defendant in exchange for enrolling in classes, applying for enrollment, or obtaining employment at Defendant, they

entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any PII that it was no longer required to maintain.

176. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

177. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

178. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

179. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, and were consistent with industry standards.

180. Plaintiff and Class Members paid money and/or provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

181. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

182. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

183. Plaintiff and Class Members fully and adequately performed their obligations

under the implied contracts with Defendant.

184. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII or to destroy it once it was no longer necessary to retain the PII.

185. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

186. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

187. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

188. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

189. This count is pleaded in the alternative to the Breach of Implied Contract claim (Count III) above.

190. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and Class Members.

191. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the

portion of each payment made that is allocated to data security is known to Defendant.

192. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII and paid money to Defendant in connection with their admission applications and/or enrollment and/or provided their labor to Defendant and/or its agents, and in so doing, provided Defendant with their PII based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiff and Class Members should have received from Defendant the goods, services, and/or employment that were the subject of the transaction and have their PII protected with adequate data security.

193. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

194. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and instead directed those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

195. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

196. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

197. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

198. Defendant obtained a benefit from Plaintiff and Class Members by fraud and/or the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiff and Class Members relied upon it to safeguard their PII against foreseeable risks.

199. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

200. Plaintiff and Class Members have no adequate remedy at law.

201. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

202. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injuries and/or harms.

203. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - 1. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - 2. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

3. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
4. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
5. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
6. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
7. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
8. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
9. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network

is compromised, hackers cannot gain access to other portions of Defendant's systems;

10. Requiring Defendant to conduct regular database scanning and securing checks;
11. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
12. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
13. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
14. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both

internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and
 16. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
- G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- H. For an award of punitive damages, as allowable by law;
- I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

- J. Pre- and post-judgment interest on any amounts awarded; and
- K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 6, 2023

Respectfully submitted,

s/ Joe Kendall

JOE KENDALL

Texas Bar No. 11260700

KENDALL LAW GROUP, PLLC

3811 Turtle Creek Blvd., Suite 1450

Dallas, Texas 75219

214-744-3000

214-744-3015 (Facsimile)

jkendall@kendalllawgroup.com

John J. Nelson*

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, LLC

280 S. Beverly Drive

Beverly Hills, CA 90212

Telephone: (858) 209-6941

Fax: (858) 209-6941

Email: jnelson@milberg.com

Attorney For Plaintiff

**Pro Hac Vice application forthcoming*